

Monge, Elaine (SCA)

12626
From: noreply@formstack.com
Sent: Monday, March 12, 2018 11:43 AM
To: Breaches, Data (SCA)
Subject: Security Breach Notifications



Formstack Submission For: Security Breach Notifications
Submitted at 03/12/18 11:42 AM

Business Name: Atwood & Moore - Attorneys at Law

Business Address:

Foreign Business Address:

Company Type: Other

Your Name: James Giszczak

Title: Member

Contact Address: McDonald Hopkins PLC
39533 Woodward Avenue, Suite 318
Bloomfield Hills, MI 48304

Foreign Contact Address:

Telephone Number: (248) 220-1354

Extension:

Email Address: jgiszczak@mcdonaldhopkins.com

Relationship to Org: Other

Breach Type:	Electronic
Date Breach was Discovered:	02/09/2018
Number of Massachusetts Residents Affected:	1
Person responsible for data breach.:	Unknown
Please give a detailed explanation of how the data breach occurred.:	On October 28, 2017, Atwood & Moore learned that an employee may have been the victim of a business email compromise. On February 9, 2018, the extensive forensic investigation and document review concluded that one Atwood & Moore employee email account had been potentially compromised and that an unknown individual may have had access, via that compromised email account, to personal information belonging to current and former clients, and some employees. The unauthorized party was potentially able to access personal information of one Massachusetts resident, including name, social security number and bank account information.
Please select the type of personal information that was included in the breached data.:	Financial Account Numbers = Selection(s) Social Security Numbers = Selection(s)
Please check ALL of the boxes that apply to your breach.:	The breach was a result of a malicious/criminal act. = Selection(s)
For breaches involving paper: A lock or security mechanism was used to physically protect the data.:	N/A
Physical access to systems containing personal information was restricted to authorized personnel only.:	N/A
Network configuration of breached system:	Internet Access Available

For breaches involving electronic systems, complete the following:

Personal information stored on the breached system was password-protected and/or restricted by user permissions. = Selection(s)

All Massachusetts residents affected by the breach have been notified of the breach.:

Yes

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply)::

US Mail = Selection(s)

Date notices were first sent to Massachusetts residents (MM/DD/YYYY):

03/09/2018

All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services .:

Yes

Law enforcement has been notified of this data breach.:

No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring.:

Since learning of the possible breach, Atwood & Moore conducted an internal investigation and forensic investigation, notified the affected Massachusetts resident, and offered credit monitoring services to the affect resident. Further, Atwood and Moore took rest the passwords for all users involved, as well as for all employees. Atwood and Moore provided updated training to all employees regarding recognizing and avoiding phishing attacks. Atwood and Moore uses an outside information technology firm to monitor its systems and network traffic for potentially malicious activity.

Copyright © 2018 Formstack, LLC. All rights reserved. This is a customer service email.

Formstack, 8604 Allisonville Road, Suite 300, Indianapolis, IN 46250

Monge, Elaine (SCA)

From: Czuprynski, Christine <cczuprynski@mcdonaldhopkins.com>
Sent: Monday, March 12, 2018 11:45 AM
To: Breaches, Data (SCA)
Subject: Security Breach Notification
Attachments: Atwood and Moore -- Notification to MA OCABR (7268075x7AB84).pdf; Atwood and Moore -- MA Template Notice Ltr (7268008x7AB84).pdf

To Whom it May Concern:

Attached please find the security breach notification submitted online on behalf of Atwood & Moore. Attached also please find the notice letter template for the impacted Massachusetts resident.

Thank you,
Chris

Christine Czuprynski
Counsel

T: 248.220.1360
cczuprynski@mcdonaldhopkins.com
www.mcdonaldhopkins.com

39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

McDonald Hopkins
A business advisory and advocacy law firm®



Data Breach Notification Submission

Data Breach Notification Submission

Instructions: Please complete the form below to submit a data breach notification to the Office of Consumer Affairs and Business Regulation. You can also print this submission for your own records. Please note under M.G.L. C93H, a separate notification must be sent to the Attorney General's Office.

If you're mailing your submission, please send to: Office of Consumer Affairs and Business Regulation, 501 Boylston St., Suite 5100, Boston, MA 02116

- Individual breaches affecting multiple debit/credit card holders of your organization can be reported on a monthly basis.
- Please do not include any personally identifiable information for Massachusetts residents in any of the fields.

Section I: Organization & Contact Information

Business Name*

Atwood & Moore - Attorneys at Law

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

52

[illegible]

Other ☐

James

Giszczak

3/12/2018

Title *

Member

Contact Address (optional)

McDonald Hopkins PLC

39533 Woodward Avenue, Suite 318

Bloomfield Hills

City

Michigan



State

48304

ZIP Code

Foreign Contact Address (optional)

If your contact address is outside the United States, enter the address here

Telephone Number *

(248) 220-1354

Extension (optional)

Email Address *

jgiszczak@mcdonaldhopkins.com

Relationship to Org *

Other



Section II: Breach Information

Breach Type *

Electronic



Date Breach was Discovered *

02



09



2018



Number of Massachusetts Residents Affected *

1

Person responsible for data breach. *

Unknown



Please give a detailed explanation of how the data breach occurred. *

On October 28, 2017, Atwood & Moore learned that an employee may have been the victim of a business email compromise. On February 9, 2018, the extensive forensic investigation and document review concluded that one Atwood & Moore employee email account had been potentially compromised and that an unknown individual may have had access, via that compromised email account, to personal information belonging to current and former clients, and some employees. The unauthorized party was potentially able to access personal information of one Massachusetts resident, including name, social security number and bank account information.

Please select the type of personal information that was included in the breached data. *

	Selection(s)
Financial Account Numbers	<input checked="" type="checkbox"/>
Social Security Numbers	<input checked="" type="checkbox"/>
Driver's License	<input type="checkbox"/>
Credit/Debit Card Number	<input type="checkbox"/>

Please check ALL of the boxes that apply to your breach. *

	Selection(s)
The person(s) with possession of personal information had authorized access	<input type="checkbox"/>
The breach was a result of a malicious/criminal act.	<input checked="" type="checkbox"/>
The breach occurred while the data was being transported outside of your premises.	<input type="checkbox"/>
The breach occurred at the location of a third party service provider.	<input type="checkbox"/>

There is a written contract in place with the third-party provider
requiring protection of personal information.

☐

Section III: Security Environment

For breaches involving paper: A lock or security mechanism was used to physically protect the data. *

☐ Yes

☐ No

☒ N/A

Physical access to systems containing personal information was restricted to authorized personnel only. *

☐ Yes

☐ No

☒ N/A

Network configuration of breached system *

Internet Access Available ☒

For breaches involving electronic systems, complete the following *

	Selection(s)
Breached data was encrypted.	<input type="checkbox"/>
The key to encrypted data was stolen.	<input type="checkbox"/>

Personal information stored on the breached system was password-protected and/or restricted by user permissions.	<input checked="" type="checkbox"/>
N/A	<input type="checkbox"/>

Section IV: Remediation

All Massachusetts residents affected by the breach have been notified of the breach. *

☒ Yes

☐ No

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply): *

	Selection(s)
E-mail	<input type="checkbox"/>
US Mail	<input checked="" type="checkbox"/>
Online posting	<input type="checkbox"/>
TV/Radio publication	<input type="checkbox"/>
Other	<input type="checkbox"/>

Date notices were first sent to Massachusetts residents (MM/DD/YYYY) *

03 <input type="checkbox"/>	09 <input type="checkbox"/>	2018 <input type="checkbox"/>	
-----------------------------	-----------------------------	-------------------------------	---

All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services . *

☒ Yes

☐ No

Law enforcement has been notified of this data breach. *

☐ Yes

☒ No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring. *

Since learning of the possible breach, Atwood & Moore conducted an internal investigation and forensic investigation, notified the affected Massachusetts resident, and offered credit monitoring services to the affect resident. Further, Atwood and Moore took rest the passwords for all users involved, as well as for all employees. Atwood and Moore provided updated training to all employees regarding recognizing and avoiding phishing attacks. Atwood and Moore uses an outside information technology firm to monitor its systems and network traffic for potentially malicious activity.

- Any documents pertaining to the data breach including the letter being sent to the Massachusetts residents must be sent via email to data.breaches@state.ma.us
- Please do not include any personally identifiable information for Massachusetts residents in any email attachment.
- Individual breaches affecting multiple debit/credit card holders of your organization can be reported on a monthly basis.
- Please review the information you have entered and click on the "Submit Form" button below.

SUBMIT FORM

Atwood & Moore – Attorneys at Law

Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

I am writing with important information regarding a recent security incident. The privacy and security of the personal information belonging to our employees and contractors is of the utmost importance to Atwood & Moore. As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

We recently learned of a security incident that impacted Atwood & Moore's computer network. Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we worked very closely with external cybersecurity professionals. Since completing our investigation, we concluded that an unknown individual may have had access to personal information belonging to our clients. We discovered on February 9, 2018, that the compromised information included your full name, bank account information, and Social Security number.

We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

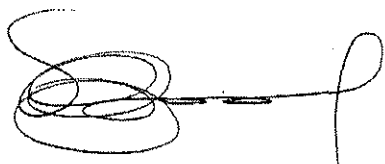
Securing your personal information is important to us. As a precautionary measure to safeguard your information from potential misuse, we have partnered with TransUnion Interactive, a subsidiary of TransUnion® to provide its myTrueIdentity online credit monitoring service for one year at no charge to you. A description of this product is provided in the attached material, which also contains instructions about how to enroll (including your personal activation code). If you choose to take advantage of this product, it will provide you with a notification of any changes to your credit information, up to \$1,000,000 Identity Theft Insurance Coverage and access to your credit report. You must complete the enrollment process by June 15, 2018.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Because your bank account information was impacted, we recommend that you contact your financial institution to inquire about steps you can take to further protect your account, including changing your account number. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 877-551-1811. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 9 a.m. to 9 p.m. Eastern time.

Sincerely,

A handwritten signature in black ink, appearing to be 'B. Jo Atwood'. It features a large, stylized 'B' with a horizontal line extending to the right, ending in a small loop.

B. Jo Atwood
Atwood & Moore

A handwritten signature in black ink, appearing to be 'Mark S. Moore'. It is written in a cursive style with the first letters of the first and last names being capitalized and prominent.

Mark S. Moore
Atwood & Moore

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary 12-Month Credit Monitoring.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code" enter the following 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

You can sign up for the online credit monitoring service anytime between now and <<Enrollment Date>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<6 digit pass code>> to speak to a TransUnion representative about your identity theft issue.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-685-1111

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/securityfreeze>
1-888-909-8872

- Your full name (first, middle, last including applicable generation, such as JR., SR., II, III, etc.)
- Your Social Security number
- Your date of birth (month, day and year)
- Your complete address including proof of current address, such as a current utility bill, bank or insurance statement or telephone bill
- If you have moved in the past five (5) years, give your previous addresses where you have lived for the past five (5) years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- Include applicable fee (\$5.00). Call or visit each of the credit reporting company websites listed above for information on fees for Security Freeze services. Forms of payment are check, money order, or credit card (American Express, Discover, MasterCard and Visa), or a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit file report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) **and** the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to remove the security freeze.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) **and** the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and monitoring free credit reports for any unauthorized activity. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC and/or the Attorney General's office in your state. You can obtain information from these sources about the steps individuals can take to protect themselves from identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at <https://www.identitytheft.gov/>, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. Obtaining a Police Report.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this issue. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.